

Young people, privacy and trust in Slovenia: the case for stronger regulations

May 2023

Katja K. Ošljak & Rys Farthing

Executive Summary

Young people's digital lives in Slovenia can be rich and rewarding, but they can also leave large data footprints that create commercial risks. This research explores young people's data footprints and their perspectives about trust and technology, as well as the reforms they want to improve their privacy. It finds that:

- In a survey of over 3,000 young people in primary and secondary schools around Slovenia,¹ a third of young people report they do not trust how their data is collected, and a third report that they are unable to check what data is collected about them
- Young people's data is routinely collected by apps used in schools. An analysis of apps frequently used in schools and by Slovenian children found that young people are frequently tracked 'outside the classroom' by products used in schools.
- Young people want stronger protections for their privacy in regulation. Workshops with over 15,000 young people found that young people want wide ranging improvements ranging from less data collection, to stronger data security, to an end to excessive data retention.

Combined, this suggests a critical role for data protections to advance their rights in an increasingly digital Slovenia. As part of the European Union, Slovenia needs to develop strong, enforceable guidelines around the protection of young people's data.

¹ University of Ljubljana 2022 *Youths' media repertoires: Social, political and cultural aspects of digitized everyday life* (online survey, J5-2564). Survey active for primary school students from March 10 to June 24, 2022, and for secondary school students from April 13 to June 24, 2022, last entry on June 23, 2022. More about the research [available at www.medijimladih.si](http://www.medijimladih.si)

Contents

Introduction	1
A trust and awareness gap: Results from a country wide survey	4
The datafication of young Slovenians: An analysis of digital products frequently used.	7
What young people want to happen with their data: Results from workshopping ideal “rules” around privacy	10
Appendix	16
1. Additional trust gap data	16
2. Additional awareness gap data	20

Introduction

Advancing young people's rights in an increasingly digital Slovenia requires realizing their right to privacy and data protection. This is not a trivial nor niche concern.

Children grow up in a 'datafied' Slovenia. Data is collected about children before they take their first breath — pregnancy apps, heartbeat monitors and ultrasounds shared on social media all process their data in utero. And this collection continues right through childhood; from AI enabled baby monitors to connected toys to fitness apps for teens. As the COVID-19 pandemic showed, many of the day-to-day experiences of children will now be routinely digitised and datafied, and the amount of data that is now collected about young Slovenians is immense.

The way young people's data is collected and used present risks to children's rights in the digital environment. As the UN Committee on the Rights of the Child outlined:

The digital environment includes businesses that rely financially on processing personal data to target revenue-generating or paid-for content, and such processes intentionally and unintentionally affect the digital experiences of children. Many of those processes involve multiple commercial partners, creating a supply chain of commercial activity and the processing of personal data that may result in violations or abuses of children's rights, including through advertising design features that anticipate and guide a child's actions towards more extreme content, automated notifications that can interrupt sleep or the use of a child's personal information or location to target potentially harmful commercially driven content.²

These risks are evident in Slovenia, with this data collection violating young people's right to privacy and often used to fuel products that can harm them. In a recent event hosted by Vsak Institute, Facebook whistleblower Frances Haugen stressed for example:

- The mental health risks that platforms like Instagram pose. Instagram has internal research that shows Instagram is uniquely harmful to young people but has failed to act. Research has shown that many of these risks are exacerbated by the use of children's data to profile them³.

² Paragraph 40, United Nations Committee on the Rights of the Child 2021 [General Comment 25 on Children's Rights in Relation to the Digital Environment](#)

³ For example, Facebook and Instagram both use children's data to profile them in potentially risky ways for advertising. See for example Sam Levin 2017 'Facebook told advertisers it can identify teens feeling 'insecure' and 'worthless'' *The Guardian* <https://www.theguardian.com/technology/2017/may/01/facebook-advertising-data-insecure-teens> and Dylan Williams, Alex McIntosh & Rys Farthing 2021 *Profiling Children for Advertising* Reset Australia https://au.reset.tech/uploads/resettechaustralia_profiling-children-for-advertising-1.pdf

- The impact of algorithms on young people, that can recommend content that is high risk. Ms Haugen talked about how searching for something innocuous like healthy recipes can turn into Facebook recommending pro anorexia content very quickly. Many of these algorithms are trained on, and respond to, children's data⁴.
- The risks of addiction to social media platforms, which are systemically under-reported. Again, it is children's data that is used to design and AB test these 'engagement maximising' features that lead to addictive behaviours⁵.

Further, recent evidence has shown that young Slovenian people are often unable to meaningfully consent to data collection practices in the digital world, with privacy policies for popular apps regularly being unavailable in Slovenian⁶.

Slovenia has both moral and legal obligations to ensure that young people's privacy is respected and their data protected, by all organisations that process children's data⁷.

To ensure that young people's experiences inform Slovenia's data protection regulations, this report documents young people's perspectives about trust, data and privacy, which was collected by the Better Digital Slovenia Initiative over 2022. It includes:

- Survey findings from over 3,000 young people from primary and secondary schools around Slovenia, who took part in a survey undertaken by the University of Ljubljana, exploring aspects of their digital lives⁸. This survey included questions about trust and data awareness which suggest the need for stronger regulations around the use of young people's data.
- Case studies about young people's datafication in Slovenia, including:
 - An analysis of popular technology products used in schools ('EdTech') and the data trackers often installed in these products

⁴ Two recent reports documented how Instagram's algorithm amplifies pro-anorexia eating disorder content. Tech Transparency Project 2021 [Thinstagram: Instagram's algorithm fuels eating disorder epidemic](#), and Fairplay 2022 [Designing for Disorder](#). Researchers for the later report found Slovenians in the pro-eating disorder bubble, with biographies such as '~ 📍 Slovenia (but in love with Germany 🇩🇪) ~ 💕 thinspo 💕 ~ need to be skinny ~ hw: 68kg/ cw: 57kg/ ugw: 54kg/ ugw: 51kg/ ugw: 47kg ~' Slovenians are being actively affected by Instagram's algorithm

⁵ Vikram R. Bhargava & Manuel Velasquez 2020 'Ethics of the Attention Economy: The Problem of Social Media Addiction' *Business Ethics Quarterly* DOI: <https://doi.org/10.1017/beq.2020.32>

⁶ Fairplay 2022 *Global Platforms: Partial Protections Design Discriminations* <https://fairplayforkids.org/wp-content/uploads/2022/07/design-discriminations.pdf>

⁷ Paragraph 70, UN Committee on the Rights of the Child 2021 [General Comment 25 on Children's Rights in Relation to the Digital Environment](#)

⁸ University of Ljubljana 2022 *Youths' media repertoires: Social, political and cultural aspects of digitized everyday life* (online survey, J5-2564). Survey active for primary school students from March 10 to June 24, 2022, and for secondary school students from April 13 to June 24, 2022, last entry on June 23, 2022. More about the research [available at www.medijimladih.si](http://www.medijimladih.si)

- An analysis of the social media apps and platforms that are popular among Slovenian young people, and the trackers and data these products are able to access
- Analysis of workshops with over 15,000 young people exploring privacy and trust held across Slovenia from Sept 2022 to Jan 2023 . Workshop facilitators⁹ collected young people's suggestions around improvements to privacy, ranging from wanting less data collection, stronger data security and an end to excessive data retention among others.

It concludes by calling for stronger protections for children and young people, in ways that reflect what young people themselves want; less data exploitation in the first instance, greater control, greater transparency, and to feel safer and more secure.

⁹ We would like to thank the workshop facilitators who helped us gather the research data: Anja Sotenšek, Domen Savič, Eva Djaković, Gordana Erdelić and Karmen Kovač.

A trust and awareness gap: Results from a country wide survey

Between April and June 2022, young people from over 70 different schools took part in a survey in which they were asked about how much they trusted that their data was handled with care, and if they were aware of how to check what data was collected about them. In total, 2,301 primary school students, aged 11-17 years old, and another 1,121 secondary school students, aged 15-22 years old took part, (see Appendix figures 1 and 2 for demographic details).¹⁰

Young people's trust of digital products

Nearly a thousand secondary school students responded if they trusted platforms, applications and websites to handle their data with care. 36% of young people did not trust platforms, 27% did trust platforms, and 37% were unsure about whether to trust or distrust platforms (see figure 3). This suggests a 'trust deficit' in young people's digital lives.

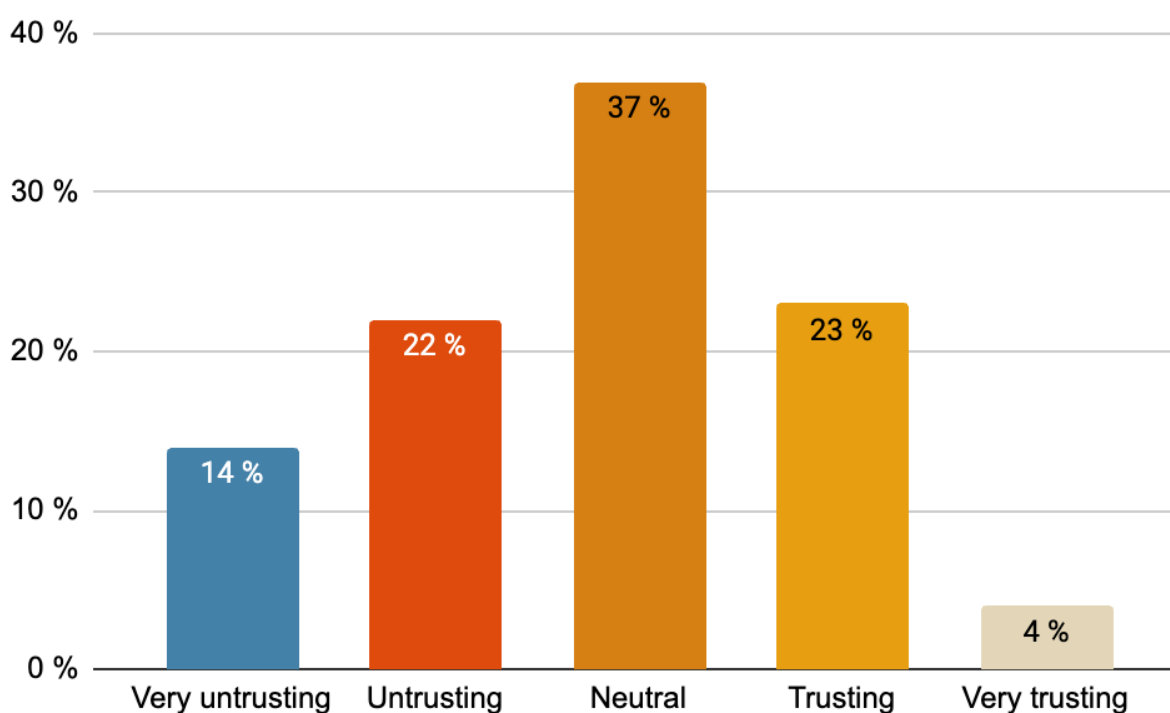


Fig 3: Responses to 'I trust (platforms, applications & social networks) to handle my data with care' (n=948)

¹⁰ University of Ljubljana 2022 *Youths' media repertoires: Social, political and cultural aspects of digitized everyday life* (online survey, J5-2564). Survey active for primary school students from March 10 to June 24, 2022, and for secondary school students from April 13 to June 24, 2022, last entry on June 23, 2022. More about the research [available at www.medijimladih.si](http://www.medijimladih.si)

We explored how different demographics affected this trust deficit:

- Age: Distrust grows with age, older young people are less trusting of platforms than 14 and 15 year-olds (see figure 4, in appendix 1).
- Gender: Young women have slightly higher levels of distrust, while non-binary young people are significantly more distrusting albeit with small sample sizes (see figure 5).
- Academic Performance: Students who are struggling or exceeding academically are more distrusting than students who report doing 'sufficiently' (see figure 6).
- Social Class: Distrust appears to grow with family capital. Young people who do not have their own room appear more trusting than students who do (see figure 7). Likewise, young people who have no books in the house or only enough to fill a bookshelf have higher levels of trust than those who have more than one book case full, although those with enough to fill one book case are the most distrusting of all (see figure 8).
- Access to Technology: Young people who do not have a computer in their home are more distrustful than those who have three or more (see figure 9).

Young people's understanding about what data is collected about them

We asked 3,090 secondary *and* primary school students if they know how to check what information apps and websites are collecting about them, in both surveys. Combined, more than a third of young people self-report that they are unable to check what data is collected about them. This lack of knowledge is indicative of a crisis of 'data awareness', and raises questions about the nature of informed consent, the legal basis for most apps and websites data collection practices.

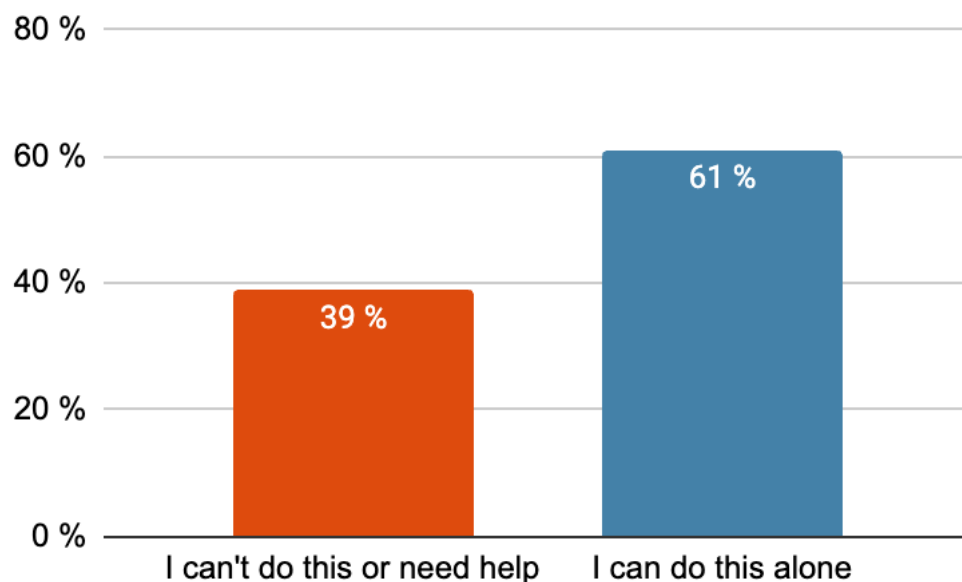


Figure 10: Young people's self-reported ability to check what information websites or apps are collecting about them (n=3,090, combined from both the elementary and secondary school samples)

We explored levels of awareness by different demographics across both surveys:

- Age: As young people age, they report slightly more data awareness, albeit with a slight dip when young people turn 18 (potentially due to a growing understanding about the complexity of the data that is collected about them). Regardless, a third of young people who are 16 and 17 years old still report not being able to check what data is collected about them without requiring help (see figure 11 in appendix 2).
- Gender: Young women reported lower levels of data awareness than young men, with 46% of girls, 32% of boys and 35% non-binary young people reporting that they would need help to check what data is collected about them (see figure 12).
- Academic Performance: Young people who reported failing grades in their last academic school year reported less data awareness, but 40% of young people who did well to excellently still reported struggling (see figure 13).
- Social Class: Class yielded mixed results. Young people who did not have their own bedrooms reported slightly less data awareness (see figure 14), but those with fewer books in their house reported a higher level of data awareness (see figure 15).
- Access to Technology: Young people with access to more computers reported higher levels of data awareness (see figure 16).

The datafication of young Slovenians: An analysis of digital products frequently used.

The trust gap and awareness deficit are particularly concerning given the ongoing datafication of young people in Slovenia. Every single day, data is harvested about young people inside and outside of the classroom, creating risks and amplifying commercial exploitation. Below we explore the datafication of young people in schools and on social media.

Datafication in schools

Products frequently used in schools across Slovenia collect data about young people that is often unnecessary, or handle it in ways that create unnecessary risk. An analysis of the privacy policies of commonly used EdTech products in schools and education institutions, as published by the University of Ljubljana,¹¹ demonstrates how they deploy cookies, tracking pixels and share data with third parties.

GeoGebra. According to their privacy policy:¹²

- The app has persistent cookies installed. These allow the app to track what a student does online after they leave the app
- The app collects student's location data "We may collect and store information about your location if you enable your computer or mobile device to send us location information"
- The app embeds a Google Analytics cookie that collects data about students IP addresses and websites accessed, and transmits it to and is by Google on servers in the United States.

Photomath. According to their privacy policy:¹³

- The app collects students location data including "IP address, satellite, cell phone tower or WiFi signals"
- Allows third party providers to access student information, and allows these third parties to also share it with third parties "We may use third-party analytics services to analyze the Service on our behalf. These service providers may use cookies*, web beacons, crash logs and other technologies to collect information about your use of the Service. These

¹¹ Mateja Bevčič *et al* 2021 *Recommendations for the equipment of schools with ICT: recommendations for the use of didactically appropriate ICT: analysis of the situation regarding the equipment of schools with ICT in selected EU countries* <https://www.dlib.si/details/URN:NBN:SI:doc-FTL6S1TV?&language=eng>

¹² GeoGebra 2020 *GeoGebra Privacy Policy* <https://www.geogebra.org/privacy>

¹³ Photomath 2022 *Photomath Privacy Policy* <https://photomath.com/en/privacypolicy/>

service providers enable us to collect, monitor and analyze data... some automatically collected data is shared with such third party service providers”.

- Allows Photomath to share student’s data with advertisers “We may disclose personal data you provide to... our business partners, such as advertising partners”

Wolfram Mathematica. According to their privacy policy:¹⁴

- The app collects student’s location data “Physical location only”
- The app is allowed to collect a stunning range of personal data “a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, Social Security number, driver's license number, passport number or other similar identifiers”
- The app allows third party advertising cookies

Moodle. According to their privacy policy:¹⁵

- Uses Google Analytics tracking Cookie “Used to send data to Google Analytics about the visitor’s device and behaviour. Tracks the visitor across devices and marketing channels”¹⁶
- Is allowed to collect and store biometric data, including profile pictures

Plickers. According to their privacy policy:¹⁷

- Aims to minimize data collection “Plickers strives to collect as little personal information about students as possible. We use this information solely to provide and improve our service”
- The app collects student’s location data “When you access the Services, we also may access, collect, monitor, and/or remotely store location data regarding the location of your device. This location data may be derived from your IP address or collected from the GPS features of your mobile device”
- The app uses cookies and tracking pixels. These allow the app to track what a student does online after they leave the app, to “ allows us to anonymously track the online usage patterns of the Services”

During the pandemic, a number of communication apps were also deployed across Slovenia. While vital to ensuring that classes continued as students stayed home, an investigation by Human Rights Watch¹⁸ also found two products that further enabled commercial surveillance.

¹⁴ Wolfram 2022 *Privacy Policy* <https://www.wolfram.com/legal/privacy/wolfram/>

¹⁵ Moodle 2022 *Privacy Notice* <https://moodle.com/privacy-notice/>

¹⁶ Moodle 2022 *Cookies Policy* <https://moodle.com/cookies-policy/>

¹⁷ Plickers 2020 *Privacy Policy* <https://help.plickers.com/hc/en-us/articles/1260804063769-Privacy-Policy>

¹⁸ Human Rights Watch 2021 *How dare they peep into my private life?*

<https://www.hrw.org/report/2022/05/25/how-dare-they-peep-my-private-life/childrens-rights-violations-governments>

Zoom:

- The HRW investigation found this app collecting student's precise location data, time of current location, last known location, coarse location & WiFi BSSID
- The investigation found this app was also collecting student's contacts' information (i.e. phone book) including their saved profile photos, and student's phone number and call logs
- The investigation found that Zoom's privacy policy was deceptive and failed to disclose the collection of student's precise location data, phone number and call logs and contacts' information, including saved photos

Microsoft Teams:

- The HRW investigation found this app collecting student's precise location data, time of current location, last known location, coarse location & WiFi BSSID
- The investigation found this app was also collecting student's contacts' information (i.e. phone book) including their saved profile photos, and student's call logs

Except Moodle classrooms, provided by Arnes, none of these products – that we were able to find – offer their privacy policies in Slovenian, adding additional concerns around the nature of informed consent for young users.

Outside of school, young people's use of apps as part of their leisure and play activities also raises concerns about datafication.

What young people want to happen with their data: Results from workshoping ideal “rules” around privacy

Over 15,000 young people took part in workshops between September 2022 and January 2023. These workshops explored young people’s privacy, their data footprint and ways they could stay safe and private online.

At these workshops we asked young people what they thought was needed to improve their privacy in the digital world. Specifically, we asked for suggestions that they wanted to share about what “the rules” for dealing with young people’s data should be. 321 suggestions were made, which help to form 17 key asks:

1. Minimize the amount of data collected about young people, and conceal it. The most popular suggestion was for less data to be collected about young people, and for it to be broadcast or shared with fewer people. Suggestions ranged from: ‘for it not to (be) visible when you’re active’ to have ‘the option to choose friends who can screenshot your post’ to ‘to not have to provide personal data on apps’.
 - Location data was noted as particularly important, with young people requesting less collection of location data, or less accurate location data. Suggestions ranged from ‘prevent location tracking’ or to ‘be able to provide different location information’.
2. Stronger data security. Young people were worried about hacking and cybersecurity, and presented plenty of suggestions from ‘Complex password requirement’ to ‘additional password protection, multiple password layers’ to ‘Private networks, VPN’.
3. Reducing the amount of time data is kept for. The third most popular set of suggestions related to data retention, with young people expressing a desire for data to be deleted when it is not needed. Specific suggestions ranged from ‘Automatic deletion of your search history on FB, Instagram and similar web apps’ to ‘When we log out, all our data is deleted’ to ‘Automatic deletion of history after one week’.
4. Safer content moderation. Young people expressed strong desires for the content they see through digital media to be safer and more age appropriate. Suggestions ranged from ‘Banning the posting of videos that encourage children to take up dangerous challenges’ to ‘Content should be filtered before being published online’ and suggestions to better moderate for fake news and fake profiles.

5. More limitations and age restrictions. There were many suggestions that improving digital privacy required limiting or age restricting certain activities. Specific suggestions ranged from reducing use from 'daily time limits' or 'limits on the amount of video posts' to better age verification and even one suggestion for 'under 16s to not use the internet'.
6. An end to advertising. There were multiple suggestions that ads should be stopped online for young people, with suggestions ranging from 'stop advertising', to 'online adverts should be banned' to 12 different requests for an 'ad-free YouTube'
7. Increased parental engagement. A number of young people also called for increased parental supervision or oversight (although it should be noted that others called for privacy from their parents). Suggestions included 'Mandatory family limit on all phones' and calls for more 'parental supervision'.
8. More transparency. There were many concerns that digital devices or platforms are spying on young people, and requests for this to stop. Young people said 'phones and apps must not listen in on conversations' and that 'apps must not process or "eavesdrop" on the content of messages exchanged through them'.
 - Transparency also included requests for the provision of apps in Slovenian language, and transparency around when young people were chatting to bots instead of humans. One young person also asked for AI support to ensure they had read the fine print in terms of service.
9. More control and options for young people. There were multiple suggestions to allow young people to have more control and options over how their data is collected, used and broadcast. Young people wanted 'the option to set permission settings for posts' for changes to that 'screenshots can only be shared with the person's consent' and even suggestions to provide paid versions of apps (so that they could use data differently).
10. More accessible games for young people. There were multiple calls for more games to be made more accessible. Young people wanted 'Free games' or for 'More games (to) work without WiFi' for example.
11. More support and help. Young people suggested that help and support were often hard to access and requested a 'support website to help you if your personal account is hacked'
12. Stop selling young people's data. Young people's asks were clear in this regard, they asked simply 'for data to not be resold'.

13. Promoting a reduction in use and periods of 'time off'. A number of young people simply wanted to take a break from digital services, and made suggestions requesting a 'daily time limit' on devices or 'for there to be a day without phones'
14. Changing phone numbers associated with accounts. A handful of young people suggested that it would be helpful if it was easier to change phone numbers associated with social media accounts.
15. Education for young people. A handful of young people requested more education in schools, specifically for the 'safe use of the internet' to be made a 'school subject'
16. More 'privacy' from those not in your phone's contacts. Three suggestions were made to limit the ability of accounts who are not in your contact list to prevent them from being able to contact young people. (Being able to change your phone number allows you to continue to access social media accounts if you lose your phone or contract, which presumably reduces fears around needing new and more social media accounts, and hacking risks).
17. Last, but definitely not least, were calls for more youth participation in the discussions around digital governance and young people. There were two requests 'for children to be in a decision-making role instead of experts and politicians'.

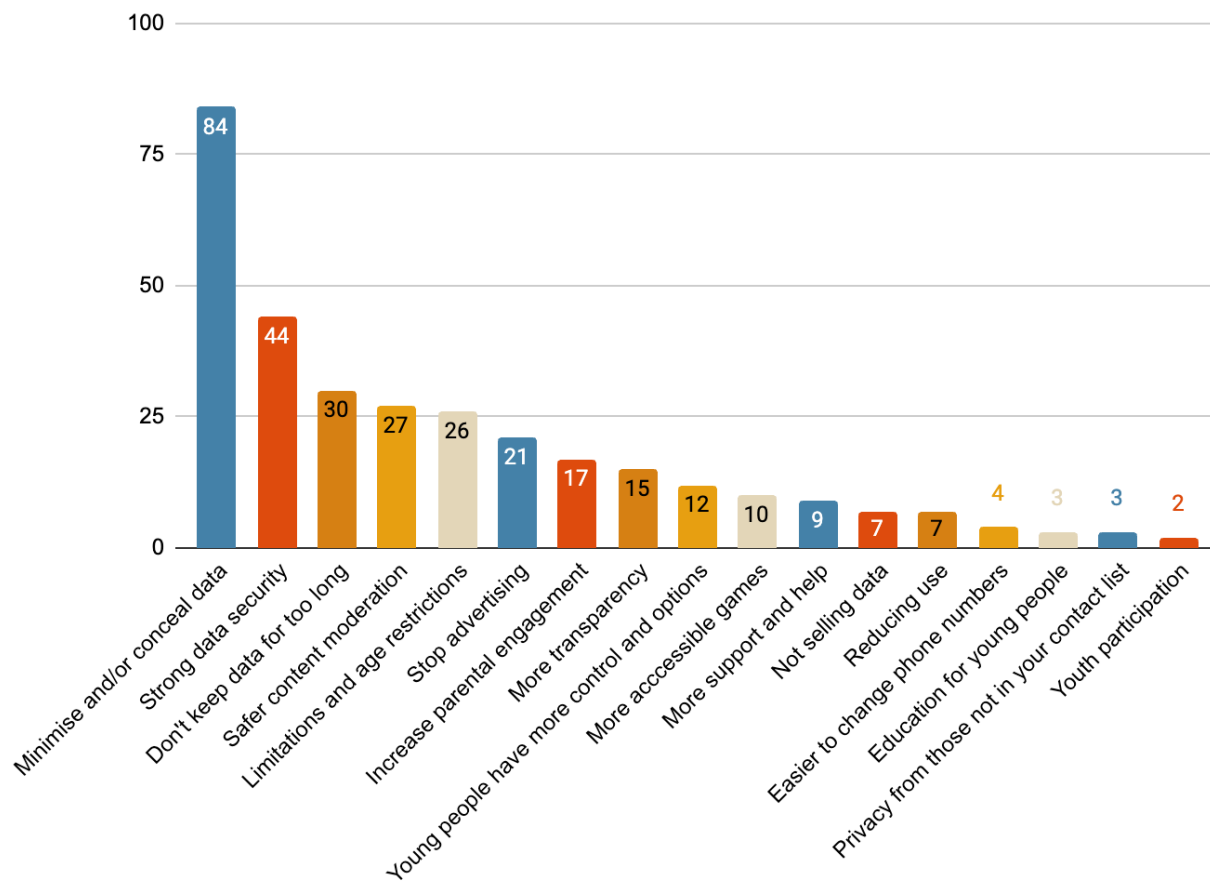


Figure 22: Young people's suggestions for 'what the rules should be' around privacy in the digital world